Attorney Docket No.: 1048-005

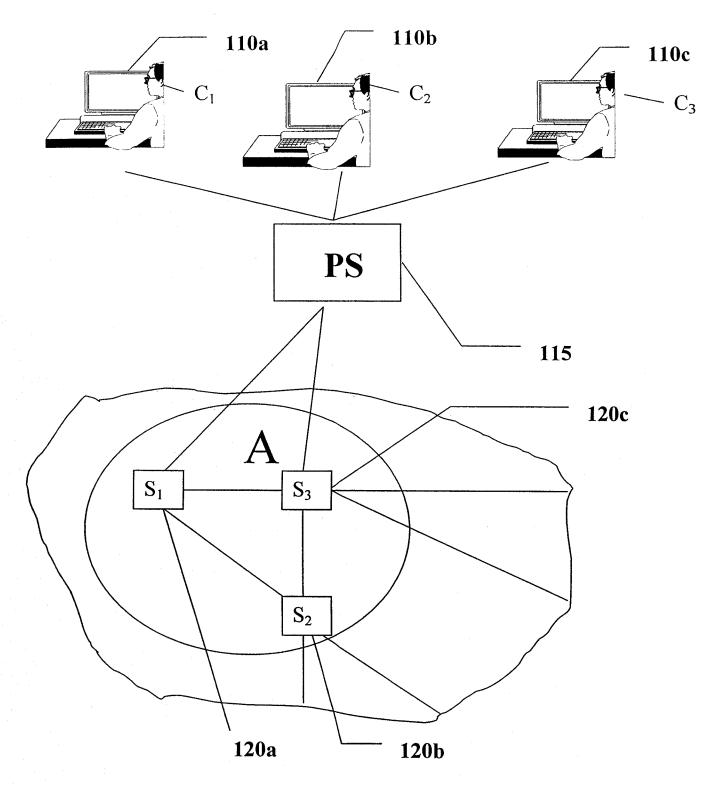


FIGURE 2

 $C_1, C_2, C_3 \leftarrow A$ 

**STEP 31** 

 $C_i$  computes  $r_i = f(P_{Ci})$ 

**STEP 32** 

 $C_i \xrightarrow{r_i} A$ 

**STEP 33** 

r<sub>i</sub> causes A to select ad<sub>i</sub>

**STEP 34** 

 $C_i \leftarrow A$ 

**STEP 35** 

$$C_1, C_2, C_3 \leftarrow f$$
PS  $\leftarrow f$ 
A STEP 41

$$C_1$$
 computes  $r_1 = f(P_{C1})$   
 $C_2$  computes  $r_2 = f(P_{C2})$   
 $C_3$  computes  $r_3 = f(P_{C3})$ 

$$C_{1} \xrightarrow{\mathbf{r}_{1}} PS$$

$$C_{2} \xrightarrow{\mathbf{r}_{2}} PS$$

$$C_{3} \xrightarrow{\mathbf{r}_{3}} PS$$

$$STEP 43$$

$$(x_1, r_1) (x_2, r_2) (x_3, r_3)$$
PS \_\_\_\_\_\_ A STEP 44

ri causes A to select adri

**STEP 45** 

$$(x_1, ad_1) (x_2, ad_2) (x_3, ad_3)$$
PS 
A STEP 46

$$C_1, C_2, C_3 \leftarrow PS$$
 STEP 47

## FIGURE 4

f

**STEP 51** 

 $C_1, C_2, C_3 \leftarrow A$ 

**STEP 52** 

 $C_1$  computes  $r_1 = f(P_{C1})$  and encrypts  $E_y[r_1]$   $C_2$  computes  $r_2 = f(P_{C2})$  and encrypts  $E_y[r_2]$  $C_3$  computes  $r_3 = f(P_{C3})$  and encrypts  $E_y[r_3]$ 

**STEP 53** 

$$C_{1} \xrightarrow{\{E_{y}[r_{1}], x_{1}\}} BB$$

$$C_{2} \xrightarrow{\{E_{y}[r_{2}], x_{2}\}} BB$$

$$C_{3} \xrightarrow{\{E_{y}[r_{3}], x_{3}\}} BB$$

STEP 54

Servers collect  $V_1 = \{ E_y[r_i], x_i \}_{i=1}^k$ 

**STEP 55** 

Servers mix  $V_1$  by random secret permutation  $\sigma_1$ 

to obtain  $V_2 = \{r_{\sigma l}(i), E_y[\sigma_1(i)]\}$ i=1

**STEP 56** 

Servers replace each  $r_j$  in  $V_2$  with  $ad_{r_j}$ 

to obtain  $V'_2 = \{ad_r, E_y[\sigma_1(i)]\}_{i=1}^k$ 

**STEP 57** 

Servers mix V'<sub>2</sub> by random secret permutation  $\sigma_2$ 

to obtain  $V_3 = \{(E_y[ad_{\sigma_2(i)}], \sigma_2(i))\}_{i=1}^k$ 

**STEP 58** 

Servers apply quorum controlled asymmetric proxy re-encryption

to obtain  $V_4 = (E_{yci}[ad_{ri}], i)_{i=1}^k$ .

STEP 59

 $C_1, C_2, C_3 \longleftarrow A$ 

**STEP 60** 

 $C_1$ ,  $C_2$ ,  $C_3$  decrypt  $E_{yci}[ad_{ri}]$  to receive  $ad_{ri}$ 

## FIGURE 5

Replacement Sheet 6 of 6

Attorney Docket No.: 1048-005

f

